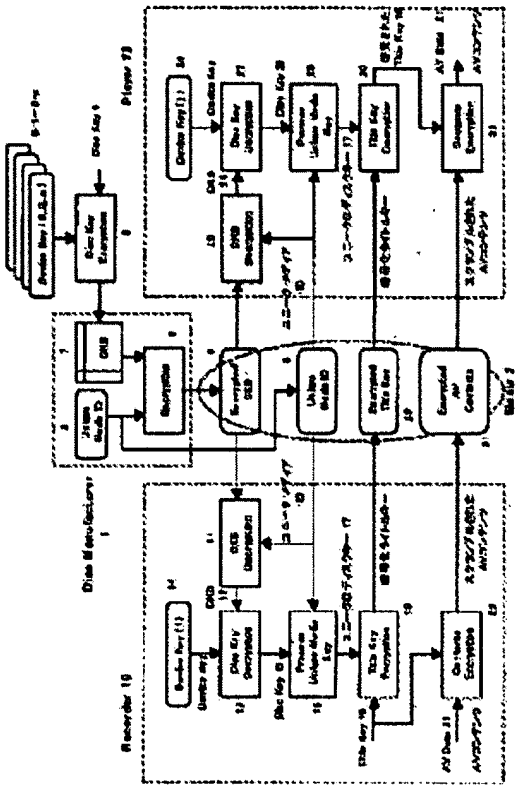
INFORMATION RECORDING MEDIUM, RECORDER, RECORDING METHOD, REPRODUCING DEVICE, REPRODUCING METHOD, RECORDING AND REPRODUCING METHOD AND TRANSMITTING METHOD

Publication number: JP2001216727
Publication date: 2001-08-10
Inventor: YOKOUCHI KENTARO
Applicant: VICTOR COMPANY OF JAPAN
Classification:
- International: ***G11B20/10;*** **G11B20/10;** (IPC1-7): G11B20/10
- European:
Application number: JP20000022128 20000131
Priority number(s): JP20000022128 20000131

Abstract of **JP2001216727**

PROBLEM TO BE SOLVED: To unnecessitate special medium structure, to make reproduction impossible when contents recorded on a recording medium is copied wholly and to normally reproduce a medium recorded by normal recording. SOLUTION: Key information in a recording medium is enciphered double and recorded in a recording medium having a characteristic ID different by each medium.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－216727
（P2001－216727A）
(43)公開日　平成13年８月10日(2001.8.10)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ１１Ｂ　20/10		Ｃ１１Ｂ　20/10	Ｈ　５Ｄ０４４

審査請求　未請求　請求項の数11　ＯＬ　（全 18 頁）

(21)出願番号　特願2000－22128(P2000－22128)

(22)出願日　平成12年１月31日(2000.1.31)

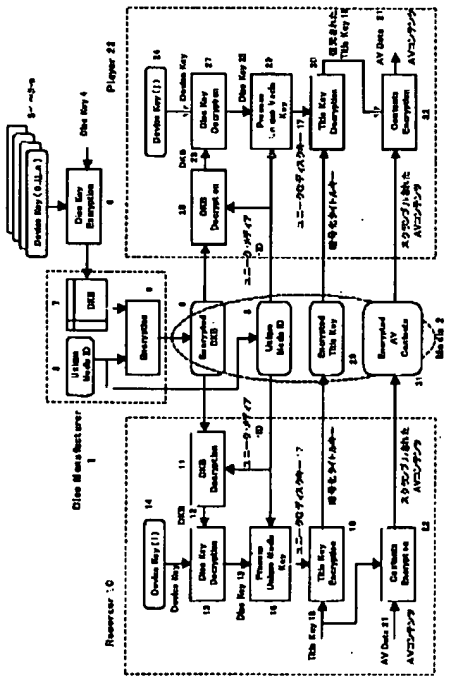
(71)出願人　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町３丁目12番地

(72)発明者　横内　健太郎
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

Ｆターム(参考)　5D044 BC02 CC04 DE50 DE57 EF05
FG18 GK17 HL08

(54)【発明の名称】　情報記録媒体、記録装置、記録方法、再生装置、再生方法、記録再生方法および伝送方法

(57)【要約】
【課題】　特殊な媒体構造が不要で、記録媒体上に記録されたコンテンツが丸ごとコピーされた場合は再生を不可能とし、正規の記録で記録された媒体は正常に再生が可能とする。
【解決手段】　一枚毎に異なる固有のＩＤを有する記録媒体に記録媒体のキー情報を二重に暗号化して記録する。



【特許請求の範囲】
【請求項１】媒体固有データが記録された書き換え不可能な非データ領域である第１の領域と、
第１のキーデータを第２のキーデータで暗号化した第１の暗号化キーデータを、さらに前記媒体固有データで暗号化した第２の暗号化キーデータが記録されている第２の領域と、
ユーザデータの記録領域である書き換え可能な第３の領域とを有することを特徴とする情報記録媒体。
【請求項２】媒体固有データが記録された書き換え不可能な非データ領域と、
第１のキーデータを第２のキーデータで暗号化した第１の暗号化キーデータを、さらに前記媒体固有データで暗号化した第２の暗号化キーデータ、およびユーザデータが記録される書き換え可能な領域とを有することを特徴とする情報記録媒体。
【請求項３】請求項１あるいは請求項２に記載の情報記録媒体において、前記媒体固有データはユニーク・メディア・ＩＤで、前記第１のキーデータは単一のディスクキーで、前記第２のキーデータは複数のデバイスキーで、前記第１の暗号化キーデータは前記ディスクキーを前記複数のデバイスキーで暗号化した暗号化ディスクキーブロックで、前記第２の暗号化キーデータは前記暗号化ディスクキーブロックを前記ユニーク・メディア・ＩＤで暗号化したユニークメディア暗号化ディスクキーブロックであることを特徴とする情報記録媒体。
【請求項４】データの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第１のキーデータを複数の第２のキーデータ群で暗号化した第１の暗号化キーデータを、さらに前記媒体固有データで暗号化した第２の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体にコンテンツを記録する記録装置であって、
前記第１の暗号化キーデータから前記第１のキーデータを復号するために予め割り当てられた前記第２のキーデータ群のうちのいずれかの復号鍵を記憶する記憶手段と、
前記情報記録媒体から前記媒体固有データを読み出す手段と、
前記情報記録媒体から前記第２の暗号化キーデータを読み出す手段と、
前記読み出した媒体固有データおよび前記読み出した第２の暗号化キーデータを用いて前記第１の暗号化キーデータを復号する第１の復号手段と、
前記復号鍵および前記復号された第１の暗号化キーデータを用いて前記第１のキーデータを復号する第２の復号手段と、
前記復号された第１のキーデータおよび前記読み出された媒体固有データから中間鍵データを生成する手段と、
記録時にユーザーが決める前記コンテンツ毎に異なる第３のキーデータを前記中間鍵データで暗号化する第１の暗号手段と、
記録する前記コンテンツを前記第３のキーデータで暗号化する第２の暗号手段と、
前記第１の暗号化手段で暗号化された前記第３のキーデータおよび前記第２の暗号化手段で暗号化された前記コンテンツを前記情報記録媒体の前記書き換え可能な領域に記録する記録手段とを有することを特徴とする記録装置。
【請求項５】データの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第１のキーデータを複数の第２のキーデータ群で暗号化した第１の暗号化キーデータを、さらに前記媒体固有データで暗号化した第２の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体にコンテンツを記録する記録方法であって、
前記記録媒体から前記媒体固有データを読み出し、
前記記録媒体から前記第２の暗号化キーデータを読み出し、
前記読み出した媒体固有データおよび前記読み出した第２の暗号化キーデータを用いて前記第１の暗号化キーデータを復号し、
前記第１の暗号化キーデータを復号するために予め割り当てられた前記第２のキーデータ群のうちのいずれかの復号鍵で前記第１の暗号化キーデータを復号して前記第１のキーデータを復号し、
前記復号された前記第１のキーデータおよび前記媒体固有データから中間鍵データを生成し、
記録時にユーザーが決める前記コンテンツ毎に異なる第３のキーデータを前記中間鍵データで第３の暗号化キーデータを生成し、
記録する前記コンテンツを前記第３の暗号化キーデータで暗号化して暗号化コンテンツを生成し、
前記第３の暗号化キーデータおよび前記暗号化コンテンツを前記情報記録媒体の前記書き換え可能な領域に記録することを特徴とする記録方法。
【請求項６】データの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第１のキーデータを複数の第２のキーデータ群で暗号化した第１の暗号化キーデータを、さらに前記媒体固有データで暗号化した第２の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体であって、
コンテンツの記録時に、前記第２の暗号化キーデータを前記媒体固有データで復号した前記第１の暗号化キーデータを、さらに予め割り当てられた前記第２のキーデータ群のうちのいずれかの復号鍵で復号した前記第１のキーデータおよび前記媒体固有データを用いて生成した中

間鍵データで記録時にユーザーが決めるコンテンツ毎に異なる第３のキーデータを暗号化した第３の暗号化キーデータと、
前記第３のキーデータを鍵として前記コンテンツを暗号化した暗号化コンテンツとが前記書き換え可能な領域に記録されていることを特徴とする情報記録媒体。
【請求項７】データの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第１のキーデータを複数の第２のキーデータ群で暗号化した第１の暗号化キーデータを、さらに前記媒体固有データで暗号化した第２の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体にコンテンツを記録するにあたり、
前記第２の暗号化キーデータを前記媒体固有データで復号した前記第１の暗号化キーデータを予め割り当てられた前記第２のキーデータ群のうちのいずれかの第１の復号鍵で復号された前記第１のキーデータおよび前記媒体固有データを用いて生成した中間鍵データで、記録時にユーザーが決めるコンテンツ毎に異なる第３のキーデータを暗号化した第３の暗号化キーデータと、
前記第３のキーデータを鍵として前記コンテンツを暗号化した暗号化コンテンツとが前記書き換え可能な領域に記録されている情報記録媒体より前記コンテンツを再生する再生装置であって、
前記第１の暗号化キーデータから前記第１のキーデータを復号するために予め割り当てられた前記第２のキーデータ群のうちのいずれかの第２の復号鍵を記憶する記憶手段と、
前記情報記録媒体から前記媒体固有データを読み出す手段と、
前記情報記録媒体から前記第２の暗号化キーデータを読み出す手段と、
前記読み出した媒体固有データおよび前記読み出した第２の暗号化キーデータを用いて前記第１の暗号化キーデータを復号する第１の復号手段と、
前記第２の復号鍵および前記復号した第１の暗号化キーデータを用いて前記第１のキーデータを復号する第２の復号手段と、
前記復号した第１のキーデータおよび前記読み出した媒体固有データから前記中間鍵データを生成する手段と、
前記書き換え可能な領域から前記第３の暗号化キーデータを読み出し、前記読み出した第３の暗号化キーデータおよび前記中間鍵データを用いて前記第３のキーデータを復号する第３の復号手段と、
前記書き換え可能な領域から前記暗号化コンテンツを読み出し、前記第３の復号化手段で復号された前記第３のキーデータおよび前記暗号化コンテンツを用いて前記コンテンツを復号する第４の復号手段とからなることを特徴とする再生装置。
【請求項８】データの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第１のキーデータを複数の第２のキーデータ群で暗号化した第１の暗号化キーデータを、さらに前記媒体固有データで暗号化した第２の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体にコンテンツを記録するにあたり、
前記第２の暗号化キーデータを前記媒体固有データで復号した前記第１暗号化キーデータを前記第２のキーデータ群のうちのいずれかの第１の復号鍵で復号された前記第１のキーデータおよび前記媒体固有データを用いて生成した中間鍵データで、記録時にユーザが決めるコンテンツ毎に異なる第３のキーデータを暗号化した第３の暗号化キーデータと、
前記第３のキーデータを鍵として前記コンテンツを暗号化した暗号化コンテンツとが前記書き換え可能な領域に記録されている情報記録媒体より前記コンテンツを再生する再生方法であって、
前記情報記録媒体から前記媒体固有データを読み出し、
前記情報記録媒体から前記第２の暗号化キーデータを読み出し、
前記読み出した媒体固有データおよび前記読み出した第２の暗号化キーデータから前記第１の暗号化キーデータを復号し、
前記第１暗号化キーデータ復号するために予め割り当てられた前記第２のキーデータ群のうちのいずれかの第２の復号鍵および前記第１の暗号化キーデータを用いて前記第１のキーデータを復号し、
前記復号した第１のキーデータおよび前記読み出した媒体固有データから前記中間鍵データを生成し、
前記中間鍵データおよび前記第３の暗号化キーデータを用いて前記第３のキーデータを復号し、
前記書き換え可能な領域から前記暗号化コンテンツを読み出し、前記復号した前記第３のキーデータおよび前記暗号化コンテンツを用いて前記コンテンツを復号することを特徴とする再生方法。
【請求項９】データの書き換え不可能な領域と、データの書き換え可能な領域とを有し、前記書き換え不可能な領域には媒体固有データが記録され、前記書き換え可能な領域には第１のキーデータを複数の第２のキーデータ群で暗号化した第１の暗号化キーデータを前記媒体固有データで暗号化した第２の暗号化キーデータが予め記録された情報記録媒体を用いた記録再生方法であって、
記録する際には、前記記録媒体より前記媒体固有データを読み出し、
前記記録媒体から前記第２の暗号化キーデータを読み出し、
前記読み出した媒体固有データおよび前記読み出した第２の暗号化キーデータを用いて前記第１の暗号化キーデ

ータを復号し、
前記第１の暗号化キーデータを復号するために予め割り当てられている前記第２のキーデータ群のいずれかの復号鍵および前記復号された第１の暗号化キーデータを用いて前記第１のキーデータを復号し、
前記復号された前記第１のキーデータおよび前記読み出された媒体固有データから中間鍵データを生成し、
記録時にユーザーが決めるコンテンツ毎に異なる第３のキーデータを前記中間鍵データで暗号化して第３の暗号化キーデータ生成し、
記録するコンテンツを前記第３のキーデータで暗号化して暗号化コンテンツを生成し、
前記第３の暗号化キーデータおよび前記暗号化コンテンツを前記記録媒体の書き換え可能な領域に記録し、
再生する際には、前記記録媒体から前記媒体固有データを読み出し、
前記記録媒体から前記第２の暗号化キーデータを読み出し、
前記読み出した前記媒体固有データおよび前記読み出した前記第２の暗号化キーデータから前記第１の暗号化キーデータを復号し、
前記第１の暗号化データを復号するために予め割り当てられた前記第２のキーデータ群のいずれかの第２の復号鍵および前記復号された第１の暗号化キーデータを用いて前記第１のキーデータを復号し、
前記復号した第１のキーデータおよび前記読み出した媒体固有データより前記中間鍵データを生成し、
前記記録媒体の書き換え可能な領域から読み出した前記第３の暗号化キーデータおよび前記中間鍵データを用いて前記第３のキーデータを復号し、
前記記録媒体の書き換え可能な領域から読み出した前記暗号化コンテンツおよび前記復号した第３のキーデータを用いて前記コンテンツを復号することを特徴とする記録再生方法。
【請求項１０】データの書き換え不可能な領域には、予め媒体固有データが記録されており、
データの書き換え可能な領域には、第１のキーデータを複数の第２のキーデータ群で暗号化した第１の暗号化キーデータを、さらに前記媒体固有データで暗号化した第２の暗号化キーデータが予め記録されており、
前記書き換え不可能な領域から前記媒体固有データ、前記書き換え可能な領域から第２の暗号化キーデータを伝送し、
前記伝送された媒体固有データおよび前記伝送された第２の暗号化キーデータを用いて前記第１の暗号化キーデータを復号し、
予め割り当てられた前記第２のキーデータ群のうちのいずれかのキーデータである復号鍵および前記復号された第１の暗号化キーデータを用いて前記第１のキーデータを復号し、
前記復号された前記第１のキーデータおよび前記伝送された媒体固有データから中間鍵データを生成し、
前記中間鍵データで記録時にユーザーが決めるコンテンツ毎に異なる第３のキーデータを暗号化して第３の暗号化キーデータ生成し、
前記第３のキーデータで前記コンテンツを暗号化して暗号化コンテンツを生成し、
前記第３の暗号化キーデータおよび前記暗号化コンテンツを前記書き換え可能な領域に伝送することを特徴とする伝送方法。
【請求項１１】データの書き換え不可能な領域には、予め媒体固有データが記録されており、
データの書き換え可能な領域には、第１のキーデータを複数の第２のキーデータ群で暗号化した第１の暗号化キーデータを、さらに前記媒体固有データで暗号化した第２の暗号化キーデータが予め記録されており、
前記書き換え不可能な領域から前記媒体固有データ、前記書き換え可能な領域から第２の暗号化キーデータを伝送し、
前記伝送された媒体固有データおよび前記伝送された第２の暗号化キーデータを用いて前記第１の暗号化キーデータを復号し、
予め割り当てられた前記第２のキーデータ群のうちのいずれかのキーデータである第１の復号鍵および前記復号された第１の暗号化キーデータを用いて前記第１のキーデータを復号し、
前記復号された前記第１のキーデータおよび前記伝送された媒体固有データから中間鍵データを生成し、
前記中間鍵データで記録時にユーザーが決めるコンテンツ毎に異なる第３のキーデータを暗号化して第３の暗号化キーデータ生成し、
前記第３のキーデータで前記コンテンツを暗号化して暗号化コンテンツを生成し、
前記第３の暗号化キーデータおよび前記暗号化コンテンツを前記書き換え可能な領域に伝送し、
前記書き換え不可能な領域から前記媒体固有データ、前記書き換え可能な領域から前記第２の暗号化キーデータ、前記第３の暗号化キーデータおよび前記暗号化コンテンツを伝送し、
前記伝送された前記媒体固有データおよび前記伝送された前記第２の暗号化キーデータを用いて前記第１の暗号化キーデータを復号し、
予め割り当てられた前記第２のキーデータ群のうちのいずれかのキーデータである第２の復号鍵および前記復号された第１の暗号化キーデータを用いて前記第１のキーデータを復号し、
前記復号した第１のキーデータおよび前記伝送された媒体固有データより前記中間鍵データを生成し、
前記中間鍵データおよび前記伝送された第３の暗号化キーデータを用いて前記第３のキーデータを復号し、

前記復号した第３のキーデータおよび前記伝送された暗号化コンテンツを用いて前記コンテンツを復号することを特徴とする伝送方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、高密度で大容量の記録再生が可能な情報記録媒体に対して相対運動をさせて情報を書き込み、読み出す記録再生装置（ドライブ）に用いられる情報記録媒体、記録装置、記録方法、再生装置、再生方法、記録再生方法、および伝送方法に関する。

【０００２】

【従来の技術】情報記録媒体として、ＤＶＤが登場しているが、これらに記録されている情報はデジタル情報であるため、デジタル情報が容易にコピーできる状態にあると複製物を劣化なく生成でき、著作権者の権利を侵害するおそれがあるため、コピー防止に関して種々方法が従来提案されている。

【０００３】例えば、ＤＶＤ－Ｖｉｄｅｏ（読み出し専用）でのコピーガードに関しては、ＤＶＤのコピー防止の基本になる方式であるＣＳＳ（Ｃｏｎｔｅｎｔ Ｓｃｒａｍｂｌｅ Ｓｙｓｔｅｍ）が提案されている。ＣＳＳに関しては、例えば、Ｎａｔｉｏｎａｌ Ｔｅｃｈｎｉｃａｌ Ｒｅｐｏｒｔ Ｖｏｌ．４３，Ｎｏ．３，（Ｊｕｎ．１９９７）１１８頁～１２２頁「ＤＶＤ著作権保護システム」等に開示されている。ＣＳＳは、デジタル情報をＤＶＤディスクに記録する際にタイトルキー（鍵）、ディスクキー（鍵）、デバイスキー（鍵）の３層の暗号化技術を使用して暗号化し、ライセンスを受けたＣＳＳ準拠のＤＶＤ機器（プレーヤ）だけが、暗号化されたデジタル情報を復号化して再生可能とするものである。

【０００４】上記ＣＳＳに関し、ＤＶＤ－Ｖｉｄｅｏ（ＲＯＭ）への適用例ついて図６を参照して説明する。ディスク製造者（Ｄｉｓｃ Ｍａｎｕｆａｃｔｕｒｅｒ）１００は、コンテンツプロバイダーの決めるディスクキー（Ｄｉｓｃ Ｋｅｙ）１０１を複数のデバイスキー（Ｄｅｖｉｃｅ Ｋｅｙ）１０２－１から１０２－ｎによりディスクキーブロック処理部（Ｐｒｏｃｅｓｓ ＤＫＢ）１０３にて複数のディスクキー群であるディスクキーブロック（ＤＫＢ）１０４を生成する。

【０００５】これは、複数の機器が持つ異なるデバイスキー（デバイスキー１０２－１～１０２－ｎのうちの一つ）でディスクキー１０１を復号し利用できるようにするためである。次にＤＫＢ１０４をディスク１０５上の所定の領域に記録する。次にＡＶコンテンツを記録する際に決めるタイトル毎に異なるタイトルキー１０６はタイトルキー暗号化手段１０７にて、ディスクキー１０１でスクランブルされ、ディスク１０５に暗号化タイトルキー（Ｅｎｃｒｙｐｔｉｏｎｅｄ ＴｉｔｌｅＫｅｙ）１０８として記録される。また、記録されるＡＶコンテンツ１０９はコンテンツ暗号化手段（Ｃｏｎｔｅｎｔｓ Ｅｎｃｒｙｐｔｉｏｎ）１１０にて、記録する際に決められるタイトル毎に異なるタイトルキー１０６（スクランブルされる前の）でスクランブルされた暗号化ＡＶコンテンツ（Ｅｎｃｒｙｐｔｅｄ ＡＶ Ｃｏｎｔｅｎｔｓ）１０９としてディスク１０５に記録される。ディスク製造者１００は、この状態のディスク１０５を販売する。

【０００６】次にディスク１０５の再生について説明する。再生装置１１０にもあらかじめ複数のデバイスキー１０２－１～１０２－ｎのうち１つである、例えば、１０２－ｊが割り当てられている。再生装置１１０は再生に先立ち、ディスク２よりディスクキーブロック(ＤＫＢ)１０４を読み出し、ディスクキー復号部（Ｄｉｓｃ Ｋｅｙ Ｄｅｃｒｙｐｔｉｏｎ）１１１においてデバイスキー１０２－ｊでディスクキーブロック（ＤＫＢ）１０４を復号してディスクキー１０１を得る。次にディスクキー１０１でスクランブルされ、ディスク１０５に記録されている暗号化タイトルキー１０８を読み出し、タイトルキー復号部（Ｔｉｔｌｅ ＫｅｙＤｅｃｒｙｐｔｉｏｎ）１１２ではディスクキー復号部（Ｄｉｓｃ ＫｅｙＤｅｃｒｙｐｔｉｏｎ）１１１より出力されるディスクキー１０１を用いて元々のタイトルキー１０６を復号する。次に、ディスク１０５からタイトルキー１０６でスクランブルされている暗号化ＡＶコンテンツ１０９を読み出し、コンテンツ復号部（Ｃｏｎｔｅｎｔｓ Ｅｎｃｒｙｐｔｉｏｎ）１１３は復号された元々のタイトルキー１０６を使用してデスクランブルを行いＡＶコンテンツ１０９を復元して、ＡＶコンテンツを再生する。

【０００７】上述したＣＳＳはＤＶＤ－Ｖｉｄｅｏ（ＲＯＭ）等の読み出し専用媒体のみに適用可能な方法であり、ＤＶＤ－ＲＡＭ、ＤＶＤ－ＲＷ等の書き換え可能な情報記録媒体やＤＶＤ－Ｒ等の１度だけ書き込みのみ可能な情報記録媒体には適用することはできない。書き換え可能な情報記録媒体であるＤＶＤ－ＲＡＭに対しては上述したＣＳＳとは別のコピーガードシステムが提案されている。ＤＶＤ－ＲＡＭはＲＯＭ（読み出し専用）領域とＲＡＭ（書き換え可能）領域とをそなえており、コピーガードのキーとなる情報であるＤＫＢはＲＯＭの領域に予め記録されているので、重ね書きや改変できない。

【０００８】ＤＶＤ－ＲＡＭのコピーガードシステムの概要について図７を参照して説明する。ブランクメディア（記録前の情報記録媒体）に関して説明する。ディスク製造者（Ｄｉｓｃ Ｍａｎｕｆａｃｔｕｒｅｒ）２００はディスク（Ｍｅｄｉａ）２０１一枚毎に異なるユニーク・メディア・ＩＤ（Ｕｎｉｑｕｅ ＭｅｄｉａＩＤ）２０２を記録する。次にコンテンツプロバイダーの決めるディスクキー２０３を複数のデバイスキー２０４

－1から２０４－ｎによりディスクキー暗号化部（Ｄｉｓｃ　Ｋｅｙ　Ｅｎｃｒｙｐｔｉｏｎ）２０５でスクランブル（暗号化）して複数のディスクキー群であるディスクキーブロック（ＤＫＢ）２０６を生成する。これは、複数の機器が持つ異なるデバイスキーでディスクキーを復号し利用できるようにするためである。生成したＤＫＢ２０６は、ユニーク・メディア・ＩＤ２０２と共にディスク２０１上の所定の領域に記録される。ディスク製造者２００は、この状態のディスク２０１をブランクディスクとして販売する。次にコンテンツの記録について説明する。記録装置２０７にはあらかじめ複数のデバイスキー２０４－１～２０４－ｎのうち1つデバイスキー２０４－ｊが割り当てられている。最初、記録装置２０７は記録に先立ちディスク２０１一枚毎にユニークなデータ（ユニーク・メディア・ＩＤ）２０２を読み出す。同様に、ディスク２０１の所定の領域に記録されているディスクキー群(ディスクキーブロック（ＤＫＢ２０６）)を読み出す。記録装置２０７にあるディスクキー復号部（Ｄｉｓｃ　Ｋｅｙ　Ｄｅｃｒｙｐｔｉｏｎ）２０８でその装置の持つデバイスキー２０４－ｊでディスクキーブロック（ＤＫＢ）２０６を復号してディスクキー２０３を得る。復号されたディスクキー２０３はユニークメディアキー処理部（Ｐｒｏｃｅｓｓ　Ｕｎｉｑｕｅ　Ｍｅｄｉａ　Ｋｅｙ）２０９にて、先に読み出されたユニーク・メディア・ＩＤ２０２で処理され、ディスク２０１一枚毎にユニークなディスクキー２０２とされる。

【０００９】ＡＶコンテンツを記録する際に決めるタイトル毎に異なるタイトルキー２１０はタイトルキー暗号化部２１１にて、ユニークなディスクキー２０２でスクランブルされ、ディスク２０１に暗号化タイトルキー（ＥｎｃｒｙｐｔｉｏｎｅｄＴｉｔｌｅ　Ｋｅｙ）２１２として記録される。

【００１０】また、記録されるＡＶコンテンツ２１３はコンテンツ暗号化手段２１４にて、記録する際に決められるタイトル毎に異なるタイトルキー２１０でスクランブルされた暗号化ＡＶコンテンツ（Ｅｎｃｒｙｐｔｅｄ　ＡＶ　Ｃｏｎｔｅｎｔｓ）２１５としてディスク２０１に記録される。次に記録されたコンテンツの再生について説明する。再生装置２１６にもあらかじめ複数のデバイスキー２０４－１～２０４－ｎのうち1つの、例えば、２０４－ｋが割り当てられている。ここで、ディスクキーブロック（ＤＫＢ）２０６は1つのディスクキー２０３を複数のデバイスキー２０４－１～２０４－ｎで暗号化（Ｅｎｃｒｙｐｔ）しているので、再生装置２１６デバイスキー２０４－ｋと記録装置のデバイスキー２０４－ｊと異なっても復号化等には問題はない。ディスクキー復号部（Ｄｉｓｃ　ＫｅｙＤｅｃｒｙｐｔｉｏｎ）２１７でデバイスキー２０４－ｋでディスクキーブロック（ＤＫＢ）２０６を復号してディスクキー２０３を得る。復号されたディスクキー２０３は記録側で使ったディスク２０１一枚毎にユニークなディスクキー２０２と一致させるため、ディスク２０１より読み出されたユニーク・メディア・ＩＤ２０２でユニークメディアキー処理部（Ｐｒｏｃｅｓｓ　ＵｎｉｑｕｅＭｅｄｉａ　Ｋｅｙ）２１８で処理され、ユニークなディスクキー２０２を得る。次にディスク２０１に記録されているユニークなディスクキー２０２でスクランブルされている暗号化タイトルキー２１２を読み出し、タイトルキー復号部（Ｔｉｔｌｅ　Ｋｅｙ　Ｄｅｃｒｙｐｔｉｏｎ）２１９にてユニークメディアキー処理部（Ｐｒｏｃｅｓｓ　Ｕｎｉｑｕｅ　Ｍｅｄｉａ　Ｋｅｙ）２１８より出力されるユニークなディスクキー２０２を用いて元々のタイトルキー２１０を復号する。タイトルキー２１０でスクランブルされ記録されているＡＶコンテンツ２１５をディスク２０１から読み出し、コンテンツ復号部（Ｃｏｎｔｅｎｔｓ　Ｅｎｃｒｙｐｔｉｏｎ）２２０において復号された元々のタイトルキー２１０を使用してデスクランブルを行いＡＶコンテンツ２１３を復元してＡＶコンテンツを再生する。

【００１１】ところで、書込みのみ可能な情報記録媒体であるＤＶＤ－Ｒは、ディスクの構造はＤＶＤ－ＲＷと同一の構造（メディア上は全てＲＡＭ領域）であるが、１度しか記録できない、書き換えできない構造のためＤＶＤ－ＲではＤＫＢの記録はできるが、１度しか記録できないので重ね書きや変造後のデータは利用できなくなり、ＤＶＤ－ＲＡＭと同様なシステムで違法な複製を防止できる。

【００１２】

【発明が解決しようとする課題】上述したようにＤＶＤ－ＲＡＭでは、上述したようにＲＯＭ領域とＲＡＭ領域とを分けて設定してあるので、２つの領域の特性を両立させる事が難しく、性能の両立ができないのでＲＯＭ領域とＲＡＭ領域とをで規格を別々に定義している。従ってＤＶＤ－ＲＡＭはその構造が特殊で複雑となる。

【００１３】ＤＶＤ－Ｒはメディア構造が単純なので製造は容易であるが、ただし１度しか記録できないため、記録者の使い勝手は制限される。

【００１４】書き換え可能な情報媒体であるＤＶＤ－ＲＷでは、ＤＶＤ－Ｒのような使用者にとっての制限はないが、ＤＶＤ－ＲＷのメディア上のデータ記録領域は書き換え可能であるため、ＤＶＤ－ＲＡＭやＤＶＤ－Ｒと同じコピー防止の手法はとれない。つまり、ＤＶＤ－ＲＷはＤＶＤ－ＲＡＭの様なＲＯＭ領域を持たず、ＤＶＤ－Ｒの様なライトワンス特性も持たないため、書き換え可能なＤＶＤ－ＲＷ媒体へのＤＶＤ－ＲＡＭのコピーガードシステムと同等のコピー防止を従来と同じ手法で実現することができない。

【００１５】つまり、例えば、コピーガードの方法として上述したＤＶＤ－Ｒと同一の方法を取るとＤＶＤ－Ｒ

WではＤＫＢ記録部分が書き換え可能であることからデータ重ね書きや変造によりコピーが可能となり、不正な複写を防止することができない。また、ＤＶＤ－ＲＡＭの様なＲＯＭ領域をつくるにしても、ＤＶＤ－ＲＷでは記録前の空溝特性とＲＯＭ領域を実現するためのＥｍｂｏｓｓ　Ｐｉｔとを両立させる事が難しい。どちらかの性能を優先させると他方の性能を十分設定することができない等の矛盾が生じるため、有効なコピー防止を実現することができないという問題点を有していた。

【００１６】

【課題を解決するための手段】本発明は、上述の問題点を解決するために、媒体固有データが記録された書き換え不可能な非データ領域である第１の領域と、第１のキーデータを第２のキーデータで暗号化した第１の暗号化キーデータを、さらに前記媒体固有データで暗号化した第２の暗号化キーデータが記録されている第２の領域と、ユーザデータの記録領域である書き換え可能な第３の領域とを有することを特徴とする情報記録媒体を提供する。また、本発明は、上述の問題点を解決するために媒体固有データが記録された書き換え不可能な非データ領域と、第１のキーデータを第２のキーデータで暗号化した第１の暗号化キーデータを、さらに前記媒体固有データで暗号化した第２の暗号化キーデータ、およびユーザデータが記録される書き換え可能な領域とを有することを特徴とする情報記録媒体を提供する。また、本発明は、上述の問題点を解決するためにデータの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第１のキーデータを複数の第２のキーデータ群で暗号化した第１の暗号化キーデータを、さらに前記媒体固有データで暗号化した第２の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体にコンテンツを記録する記録装置であって、前記第１の暗号化キーデータから前記第１のキーデータを復号するために予め割り当てられた前記第２のキーデータ群のうちのいずれかの復号鍵を記憶する記憶手段と、前記情報記録媒体から前記媒体固有データを読み出す手段と、前記情報記録媒体から前記第２の暗号化キーデータを読み出す手段と、前記読み出した媒体固有データおよび前記読み出した第２の暗号化キーデータを用いて前記第１の暗号化キーデータを復号する第１の復号手段と、前記復号鍵および前記復号された第１の暗号化キーデータを用いて前記第１のキーデータを復号する第２の復号手段と、前記復号された第１のキーデータおよび前記読み出された媒体固有データから中間鍵データを生成する手段と、記録時にユーザーが決める前記コンテンツ毎に異なる第３のキーデータを前記中間鍵データで暗号化する第１の暗号手段と、記録する前記コンテンツを前記第３のキーデータで暗号化する第２の暗号手段と、前記第１の暗号化手段で暗号化された前記第３のキーデータおよび前記第２の暗号化手段で暗号化された前記コンテンツを前記情報記録媒体の前記書き換え可能な領域に記録する記録手段とを有することを特徴とする記録装置を提供する。また、本発明は、上述の問題点を解決するためにデータの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第１のキーデータを複数の第２のキーデータ群で暗号化した第１の暗号化キーデータを、さらに前記媒体固有データで暗号化した第２の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体にコンテンツを記録する記録方法であって、前記記録媒体から前記媒体固有データを読み出し、前記記録媒体から前記第２の暗号化キーデータを読み出し、前記読み出した媒体固有データおよび前記読み出した第２の暗号化キーデータを用いて前記第１の暗号化キーデータを復号し、前記第１の暗号化キーデータを復号するために予め割り当てられた前記第２のキーデータ群のうちのいずれかの復号鍵で前記第１の暗号化キーデータを復号して前記第１のキーデータを復号し、前記復号された前記第１のキーデータおよび前記媒体固有データから中間鍵データを生成し、記録時にユーザーが決める前記コンテンツ毎に異なる第３のキーデータを前記中間鍵データで第３の暗号化キーデータを生成し、記録する前記コンテンツを前記第３の暗号化キーデータで暗号化して暗号化コンテンツを生成し、前記第３の暗号化キーデータおよび前記暗号化コンテンツを前記情報記録媒体の前記書き換え可能な領域に記録することを特徴とする記録方法を提供する。また、本発明は、上述の問題点を解決するためにデータの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第１のキーデータを複数の第２のキーデータ群で暗号化した第１の暗号化キーデータを、さらに前記媒体固有データで暗号化した第２の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体であって、コンテンツの記録時に、前記第２の暗号化キーデータを前記媒体固有データで復号した前記第１の暗号化キーデータを、さらに予め割り当てられた前記第２のキーデータ群のうちのいずれかの復号鍵で復号した前記第１のキーデータおよび前記媒体固有データを用いて生成した中間鍵データで記録時にユーザーが決めるコンテンツ毎に異なる第３のキーデータを暗号化した第３の暗号化キーデータと、前記第３のキーデータを鍵として前記コンテンツを暗号化した暗号化コンテンツとが前記書き換え可能な領域に記録されていることを特徴とする情報記録媒体を提供する。また、本発明は、上述の問題点を解決するためにデータの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第１のキーデータを複数の第２のキーデータ群で暗号化した第１の暗号化キーデータを、さらに前記媒体

固有データで暗号化した第２の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体にコンテンツを記録するにあたり、前記第２の暗号化キーデータを前記媒体固有データで復号した前記第１の暗号化キーデータを予め割り当てられた前記第２のキーデータ群のうちのいずれかの第１の復号鍵で復号された前記第１のキーデータおよび前記媒体固有データを用いて生成した中間鍵データで、記録時にユーザーが決めるコンテンツ毎に異なる第３のキーデータを暗号化した第３の暗号化キーデータと、前記第３のキーデータを鍵として前記コンテンツを暗号化した暗号化コンテンツとが前記書き換え可能な領域に記録されている情報記録媒体より前記コンテンツを再生する再生装置であって、前記第１の暗号化キーデータから前記第１のキーデータを復号するために予め割り当てられた前記第２のキーデータ群のうちのいずれかの第２の復号鍵を記憶する記憶手段と、前記情報記録媒体から前記媒体固有データを読み出す手段と、前記情報記録媒体から前記第２の暗号化キーデータを読み出す手段と、前記読み出した媒体固有データおよび前記読み出した第２の暗号化キーデータを用いて前記第１の暗号化キーデータを復号する第１の復号手段と、前記第２の復号鍵および前記復号した第１の暗号化キーデータを用いて前記第１のキーデータを復号する第２の復号手段と、前記復号した第１のキーデータおよび前記読み出した媒体固有データから前記中間鍵データを生成する手段と、前記書き換え可能な領域から前記第３の暗号化キーデータを読み出し、前記読み出した第３の暗号化キーデータおよび前記中間鍵データを用いて前記第３のキーデータを復号する第３の復号手段と、前記書き換え可能な領域から前記暗号化コンテンツを読み出し、前記第３の復号化手段で復号された前記第３のキーデータおよび前記暗号化コンテンツを用いて前記コンテンツを復号する第４の復号手段とからなることを特徴とする再生装置を提供する。また、本発明は、上述の問題点を解決するためにデータの書き換え不可能な領域とデータの書き換え可能な領域とを有し、媒体固有データが前記書き換え不可能な領域に記録され、第１のキーデータを複数の第２のキーデータ群で暗号化した第１の暗号化キーデータを、さらに前記媒体固有データで暗号化した第２の暗号化キーデータが前記書き換え可能な領域に予め記録されている情報記録媒体にコンテンツを記録するにあたり、前記第２の暗号化キーデータを前記媒体固有データで復号した前記第１暗号化キーデータを前記第２のキーデータ群のうちのいずれかの第１の復号鍵で復号された前記第１のキーデータおよび前記媒体固有データを用いて生成した中間鍵データで、記録時にユーザが決めるコンテンツ毎に異なる第３のキーデータを暗号化した第３の暗号化キーデータと、前記第３のキーデータを鍵として前記コンテンツを暗号化した暗号化コンテンツとが前記書き換え可能な領域に記録されている情報記録媒体より前記コンテンツを再生する再生方法であって、前記情報記録媒体から前記媒体固有データを読み出し、前記情報記録媒体から前記第２の暗号化キーデータを読み出し、前記読み出した媒体固有データおよび前記読み出した第２の暗号化キーデータから前記第１の暗号化キーデータを復号し、前記第１暗号化キーデータ復号するために予め割り当てられた前記第２のキーデータ群のうちのいずれかの第２の復号鍵および前記第１の暗号化キーデータを用いて前記第１のキーデータを復号し、前記復号した第１のキーデータおよび前記読み出した媒体固有データから前記中間鍵データを生成し、前記中間鍵データおよび前記第３の暗号化キーデータを用いて前記第３のキーデータを復号し、前記書き換え可能な領域から前記暗号化コンテンツを読み出し、前記復号した前記第３のキーデータおよび前記暗号化コンテンツを用いて前記コンテンツを復号することを特徴とする再生方法を提供する。また、本発明は、上述の問題点を解決するためにデータの書き換え不可能な領域と、データの書き換え可能な領域とを有し、前記書き換え不可能な領域には媒体固有データが記録され、前記書き換え可能な領域には第１のキーデータを複数の第２のキーデータ群で暗号化した第１の暗号化キーデータを前記媒体固有データで暗号化した第２の暗号化キーデータが予め記録された情報記録媒体を用いた記録再生方法であって、記録する際には、前記記録媒体より前記媒体固有データを読み出し、前記記録媒体から前記第２の暗号化キーデータを読み出し、前記読み出した媒体固有データおよび前記読み出した第２の暗号化キーデータを用いて前記第１の暗号化キーデータを復号し、前記第１の暗号化キーデータを復号するために予め割り当てられている前記第２のキーデータ群のいずれかの復号鍵および前記復号された第１の暗号化キーデータを用いて前記第１のキーデータを復号し、前記復号された前記第１のキーデータおよび前記読み出された媒体固有データから中間鍵データを生成し、記録時にユーザーが決めるコンテンツ毎に異なる第３のキーデータを前記中間鍵データで暗号化して第３の暗号化キーデータ生成し、記録するコンテンツを前記第３のキーデータで暗号化して暗号化コンテンツを生成し、前記第３の暗号化キーデータおよび前記暗号化コンテンツを前記記録媒体の書き換え可能な領域に記録し、再生する際には、前記記録媒体から前記媒体固有データを読み出し、前記記録媒体から前記第２の暗号化キーデータを読み出し、前記読み出した前記媒体固有データおよび前記読み出した前記第２の暗号化キーデータから前記第１の暗号化キーデータを復号し、前記第１の暗号化データを復号するために予め割り当てられた前記第２のキーデータ群のいずれかの第２の復号鍵および前記復号された第１の暗号化キーデータを用いて前記第１のキーデータを復号し、前記復号した第１のキーデータおよび前記読み出した媒体固有データより前記中間鍵データを

生成し、前記記録媒体の書き換え可能な領域から読み出した前記第３の暗号化キーデータおよび前記中間鍵データを用いて前記第３のキーデータを復号し、前記記録媒体の書き換え可能な領域から読み出した前記暗号化コンテンツおよび前記復号した第３のキーデータを用いて前記コンテンツを復号することを特徴とする記録再生方法を提供する。また、本発明は、上述の問題点を解決するためにデータの書き換え不可能な領域には、予め媒体固有データが記録されており、データの書き換え可能な領域には、第１のキーデータを複数の第２のキーデータ群で暗号化した第１の暗号化キーデータを、さらに前記媒体固有データで暗号化した第２の暗号化キーデータが予め記録されており、前記書き換え不可能な領域から前記媒体固有データ、前記書き換え可能な領域から第２の暗号化キーデータを伝送し、前記伝送された媒体固有データおよび前記伝送された第２の暗号化キーデータを用いて前記第１の暗号化キーデータを復号し、予め割り当てられた前記第２のキーデータ群のうちのいずれかのキーデータである復号鍵および前記復号された第１の暗号化キーデータを用いて前記第１のキーデータを復号し、前記復号された前記第１のキーデータおよび前記伝送された媒体固有データから中間鍵データを生成し、前記中間鍵データで記録時にユーザーが決めるコンテンツ毎に異なる第３のキーデータを暗号化して第３の暗号化キーデータ生成し、前記第３のキーデータで前記コンテンツを暗号化して暗号化コンテンツを生成し、前記第３の暗号化キーデータおよび前記暗号化コンテンツを前記書き換え可能な領域に伝送することを特徴とする伝送方法を提供する。さらに、本発明は、上述の問題点を解決するためにデータの書き換え不可能な領域には、予め媒体固有データが記録されており、データの書き換え可能な領域には、第１のキーデータを複数の第２のキーデータ群で暗号化した第１の暗号化キーデータを、さらに前記媒体固有データで暗号化した第２の暗号化キーデータが予め記録されており、前記書き換え不可能な領域から前記媒体固有データ、前記書き換え可能な領域から第２の暗号化キーデータを伝送し、前記伝送された媒体固有データおよび前記伝送された第２の暗号化キーデータを用いて前記第１の暗号化キーデータを復号し、予め割り当てられた前記第２のキーデータ群のうちのいずれかのキーデータである第１の復号鍵および前記復号された第１の暗号化キーデータを用いて前記第１のキーデータを復号し、前記復号された前記第１のキーデータおよび前記伝送された媒体固有データから中間鍵データを生成し、前記中間鍵データで記録時にユーザーが決めるコンテンツ毎に異なる第３のキーデータを暗号化して第３の暗号化キーデータ生成し、前記第３のキーデータで前記コンテンツを暗号化して暗号化コンテンツを生成し、前記第３の暗号化キーデータおよび前記暗号化コンテンツを前記書き換え可能な領域に伝送し、前記書き換え不可能な領域から前記媒体固有データ、前記書き換え可能な領域から前記第２の暗号化キーデータ、前記第３の暗号化キーデータおよび前記暗号化コンテンツを伝送し、前記伝送された前記媒体固有データおよび前記伝送された前記第２の暗号化キーデータを用いて前記第１の暗号化キーデータを復号し、予め割り当てられた前記第２のキーデータ群のうちのいずれかのキーデータである第２の復号鍵および前記復号された第１の暗号化キーデータを用いて前記第１のキーデータを復号し、前記復号した第１のキーデータおよび前記伝送された媒体固有データより前記中間鍵データを生成し、前記中間鍵データおよび前記伝送された第３の暗号化キーデータを用いて前記第３のキーデータを復号し、前記復号した第３のキーデータおよび前記伝送された暗号化コンテンツを用いて前記コンテンツを復号することを特徴とする伝送方法を提供する。

【００１７】

【発明の実施の形態】本発明は、メディア上のＤＫＢをディスク毎に変えて、ディスク毎に異なるＵｎｉｑｕｅ　Ｍｅｄｉａ　ＩＤを利用して暗号化したＤＫＢを生成して記録することにより、例えば、ＤＫＢ領域を含むディスク丸ごとコピーが行われたとしても、ディスク毎にＩＤが異なるため、記録されているコンテンツを再生することが不可能となり、不正な複製を防止することが可能となる。またメディア上のＤＫＢが重ね書きや改変された場合にもコンテンツの復号に必要なキーが正しく復元できなくなるので不正な複製は防止される。

【００１８】上述したようにＲｅａｄａｂｌｅ　Ｅｍｂｏｓｓ－ｐｉｔｔを現状では記録する技術が確立していないＤＶＤ－ＲＷに従来方式のＤＫＢ記録によるコピーガードを実現するため、ＤＶＤ－ＲＷのリードイン領域のＳｙｓｔｅｍ　Ｒｅｓｅｒｖｅｄ領域に、従来方式のＤＫＢをメディア固有のＵｎｉｑｕｅ　ＭｅｄｉａＩＤを使いさらに暗号化し、メディア個々に異なる暗号化ＤＫＢを記録する。ディスク製造者はＤＫＢをＵｎｉｑｕｅ　Ｍｅｄｉａ　ＩＤで暗号化し、工場出荷時に暗号化ＤＫＢをディスクに記録（Ｐｒｅ－ｒｅｃｏｒｄ）し、出荷する。

【００１９】記録装置はＵｎｉｑｕｅ　Ｍｅｄｉａ　ＩＤと暗号化ＤＫＢを読み出しＤＫＢを復元し従来方式により記録し、再生装置は同様にＵｎｉｑｕｅ　ＭｅｄｉａＩＤと暗号化ＤＫＢとを読み出しＤＫＢを復元して再生する。

【００２０】例えば、図８に示すようにＵｎｉｑｕｅ　Ｍｅｄｉａ　ＩＤ　Ａのディスクでは暗号化ＤＫＢ　Ａが生成されディスクに記録されているので、暗号化ＤＫＢを復号する際にはディスクにＵｎｉｑｕｅ　Ｍｅｄｉａ　ＩＤ　Ａが記録されていることが必要である。しかし、このディスクをビット・バイ・ビットでＵｎｉｑｕｅ　Ｍｅｄｉａ　ＩＤ　Ｂのディスクに記録した場合は、暗号化ＤＫＢを復号する際にディスクに記録されて

いるＵｎｉｑｕｅ　Ｍｅｄｉａ　ＩＤ　Ｂが使用されるため正しい復号ができなくなる。

【００２１】図９に示すようにディスク２にはその最内周部よりリードイン領域（Ｌｅａｄ－ｉｎ　Ａｒｅａ）、ユーザデータ領域（Ｕｓｅｒ　Ｄａｔａ　Ａｒｅａ）が順次配置されている。リードイン領域は記録再生の際の制御に使用されるデータを格納する領域であり、ユーザデータ領域は記録再生されるべきコンテンツを暗号化した暗号化コンテンツ（データ）を配置する領域である。

【００２２】リードイン領域は読み出し専用（書き換え不可能な領域）のＢＣＡ領域（ＢＣＡ　Ａｒｅａ）、読み出し／書き込みが可能（書き換え可能な領域）なシステムリザーブ領域（Ｓｙｓｔｅｍ　ｒｅｓｅｒｖｅｄ　Ａｒｅａ）、読み出し専用（書き換え不可能な領域）のコントロールデータ領域（Ｃｏｎｔｒｏｌ　ＤａｔａＡｒｅａ）から構成されている。ＢＣＡ領域には、ＢＣＡに関するデータ、つまり、ディスク２の１枚毎に異なるデータである上述したＵｎｉｑｕｅ　Ｍｅｄｉａ　ＩＤが記録されている。リザーブ領域は著作権やコピープロテクトに関する情報（データ）を記録するために用意されている領域であり、例えば、メディア固有のＵｎｉｑｕｅ　Ｍｅｄｉａ　ＩＤ（ＢＣＡ）を用いて暗号化することにより生成されるディスク２の個々に異なる暗号化ＤＫＢを記録する。

【００２３】なお、この暗号化ＤＫＢはリザーブ領域ではなく、ユーザデータ領域（書き換え可能な領域）に記録することも可能であり、また、リザーブ領域およびユーザデータ領域の両方の領域に記録してもよい。ユーザデータ領域に記録する場合は、その記録位置はリードイン領域の直後、ユーザデータ領域の最後、ユーザデータ領域の中の任意の位置などユーザデータ領域の所定の位置であり、更に複数の所定の位置に記録することも可能である。このようなユーザデータ領域への格納とリザーブ領域への格納とを併存させることも可能である。

【００２４】以下、本発明の実施例に関して図面を用いて詳しく説明する。図１は本発明の実施例を示す図である。

（１）ブランクメディア

まず、ブランクメディア（コンテンツが記録される前の情報記録媒体）に関して説明する。ディスク製造者（Ｄｉｓｃ　Ｍａｎｕｆａｃｔｕｒｅｒ）１はディスク（Ｍｅｄｉａ）２一枚毎にユニーク・メディア・データ（Ｕｎｉｑｕｅ　Ｍｅｄｉａ　ＩＤ）３をディスクに記録する。

【００２５】ユニーク・メディア・データ３を記録する際に、コンテンツプロバイダーの決めるディスクキー４を複数のデバイスキー５－１から５－ｎによりディスクキー暗号化部（Ｄｉｓｃ　Ｋｅｙ　Ｅｎｃｒｙｐｔｉｏｎ）６でスクランブル（暗号化）して複数のディスクキー群であるディスクキーブロック（ＤＫＢ）７を生成する。これは、複数の機器が持つ異なるデバイスキーでディスクキーを復号し利用できるようにするためである。

【００２６】なお、上記説明におけるスクランブルに関する処理は、例えば、図２に示すようなスクランブラー３００にて行うことができる。具体的にはキーデータを初期値にＭ系列のＰＮ乱数をＰＮ乱数発生手段３０１にて発生させ、スクランブルしたい入力データとＥＯＲ手段３０２にてＥＸ－ＯＲ（排他的論理和）をとることで処理を行う。図１に示した実施例では、キーデータとして図１に示した複数のデバイスキー５－１～５－ｎを初期値としてＰＮ乱数発生手段３０１入力してＰＮ乱数を発生させ、スクランブルしたいデータであるディスクキー４とＰＮ乱数とのＥＸ－ＯＲ（排他的論理和）処理をＥＯＲ手段３０２で行うことでディスクキー４をスクランブル処理することができる。なお、以下の説明でのスクランブル処理に関しても図２に示したスクランブラー３００を使用して処理することが可能である。

【００２７】なお、上述したＰＮ乱数発生手段３０１に関しては、例えば、図４に示すようなＰＮ乱数発生部５００を使用することができる。ＰＮ乱数発生部５００はＤフリップフロップ５０１、５０２、５０３、５０４を４回路を従属接続し、初期値をパラレルデータとしてＤフリップフロップ５０１、５０２、５０３、５０４に供給し、シリアル形式のＰＮ乱数を得ることができる。

【００２８】さらに詳細に説明すると、ＰＮ乱数発生手段３０１はＭ系列（最長線型符号系列）を用いた疑似乱数発生回路で、回路はある長さのシフトレジスターまたは遅延素子（実施例では４ビットのＤ－ＦＦ）と複数のレジスターの状態を演算してレジスターの入力に帰還する回路（実施例ではＥＯＲと反転回路）により構成される。

【００２９】Ｍ系列は後述するようにレジスターへの初期値および帰還回路の構成によりレジスターのクロック毎に出力に現れるビットパターンが異なり、最長２＾ｎ－１（２のｎ乗－１）の周期を持つ疑似乱数パターンが得られる。この特性を生かして本願の様なデータのスクランブルを始め通信分野（スペクトラム拡散方式など）に多用されている。

【００３０】上述した 図４に示したＰＮ乱数発生手段３０１はＰＮ符号長１５クロックで、例えばレジスターの初期値に「００００」ｂｉｎをロードしてクロック毎にレジスターをビットシフトすると、その出力には 図１０に示すように０に始まり１５クロックを１周期とする疑似乱数が得られる。また「１００１」ｂｉｎをロードしてクロック毎にレジスターをビットシフトすると、その出力には 図１１に示すように１に始まり１５クロックを１周期とする 表－１ とは異なるパターンの疑似乱数が得られる。

【００３１】このようにして得られた疑似乱数を図２に

示したスクランブラー３００に用いれば同じ入力データであっても出力されるデータは図１０および図１１に示すようにＰＮ乱数発生手段３０１の初期値によって異なり、図3のデスクランブラー４００のでＰＮ乱数発生手段４０１の初期値と帰還回路の構成を知らないと、正しく元のデータを復元する事はできない。これによりデータを秘匿する事が可能になる。

【００３２】また上述した実施例ではＰＮ乱数発生手段３０１のレジスタ長を４ビットとしたので疑似乱数の発生周期は１５クロックであるが、レジスタ長を更に長く、例えば、４０ビットや６４ビットにする事でＰＮ乱数発生手段３０１のパターン周期は飛躍的に長くなり、出力される疑似乱数のパターンもより複雑で長周期となり、スクランブラー３００の出力はさらに解読しにくくなり、秘匿性が高まる。

【００３３】ディスク２一枚毎にユニークなディスクキー群を作るため、ディスク２に記録されたディスク２一枚毎にユニークなデータ（ユニーク・メディア・ＩＤ）３を使用してスクランブルされた複数のディスクキー群（ディスクキーブロック（ＤＫＢ））７を暗号化手段（Ｅｎｃｒｙｐｔｉｏｎ）８にて再度スクランブルしてこの二重にスクランブルされた複数のディスクキー群である暗号化ＤＫＢ（Ｅｎｃｒｙｐｔｉｏｎｅｄ ＤＫＢ）９をディスク２上の所定の領域に記録する。このスクランブル処理は、例えば、上述した図2に示すようなスクランブラー３００を使用することができる。ディスク製造者1は、この状態のディスク２をブランクディスクとして販売する。

【００３４】（２）記録装置

記録装置１０にはあらかじめ複数のデバイスキー５－１～５－ｎのうち１つデバイスキー１４（５－ｊ）が割り当てられており、例えば、メモリー等の記憶手段に記憶されている。記録装置１０は記録に先立ちディスク２の所定領域に記録されているディスク２一枚毎にユニークなデータ（ユニーク・メディア・ＩＤ）３を読み出すと共に、ディスク２の所定の領域に記録されている暗号化ＤＫＢ９を読み出す。

【００３５】記録装置１０のスクランブルディスクキー復号手段（ＤＫＢ Ｄｅｃｒｙｐｔｉｏｎ）１１では、ディスク２より読み出した暗号化ＤＫＢ９を、ディスク２より読み出したユニーク・メディア・ＩＤ３でデスクランブルしてディスクキー群(ディスクキーブロック（ＤＫＢ１２））を得る。なお、上記説明におけるデスクランブル処理は、例えば、図3に示すようなデスクランブラーラー４００で行うことが出来る。デスクランブラー４００は図２に示したスクランブラー３００と同様にキーデータを初期値にＰＮ乱数発生部４０１にてＭ系列のＰＮ乱数を発生させ、デスクランブルしたいデータとＰＮ乱数とをＥＯＲ４０２においてＥＸ－ＯＲ（排他的論理和）処理を実行すればデータを復元（デスクランブル処理）することができる。

【００３６】図1に示した実施例では、キーデータとして図1に示したユニーク・メディア・ＩＤ３を初期値としてＰＮ乱数発生手段４０１入力してＰＮ乱数を発生させ、デスクランブルしたいデータである暗号化ＤＫＢ９とＰＮ乱数とのＥＸ－ＯＲ（排他的論理和）処理をＥＯＲ手段４０２で行うことで暗号化ＤＫＢ９をデスクランブル処理してＤＫＢ１２を復元することができる。なお、以下の説明でのデスクランブル処理に関しても図3に示したデスクランブラー４００を使用して処理することが可能である。また、上述したＰＮ乱数発生部４０１に関しては、上述したように、例えば、図4に示したＰＮ乱数発生部５００を使用することができる。

【００３７】次に記録装置１０にあるディスクキー復号手段（Ｄｉｓｃ Ｋｅｙ Ｄｅｃｒｙｐｔｉｏｎ）１３で記録装置１０の持つデバイスキー１４でディスクキーブロック（ＤＫＢ）１２（ＤＫＢ7に相当）を復号（デスクランブル）してディスクキー１５（ディスクキー4に相当）を得る。このデスクランブル処理にも、例えば、上述した図3に示したデスクランブラー３００を使用することが可能である。

【００３８】復号されたディスクキー１５はユニークメディアキー処理部（ＰｒｏｃｅｓｓＵｎｉｑｕｅ Ｍｅｄｉａ Ｋｅｙ）１６にて、先にディスク２より読み出されたユニーク・メディア・ＩＤ３で処理され、ディスク２一枚毎にユニークなディスクキー１７とされる。具体的には、例えば、図5に示すようにディスクキー復号部１３より出力されるディスクキー１５を鍵情報としてＥＯＲ６０１に入力しすると共に、ディスク２より再生されたユニーク・メディア・ＩＤ３を媒体識別情報としてＥＯＲ６０１に入力してＥＸ－ＯＲ（排他的論理和）処理を実行することで、ユニークなディスクキー１７が出力される。

【００３９】タイトルキー暗号化手段１９において、ＡＶコンテンツを記録する際に決めるタイトル毎に異なるタイトルキー１８は、ユニークなディスクキー１７でスクランブルされ、ディスク２に暗号化タイトルキー（Ｅｎｃｒｙｐｔｉｏｎｅｄ Ｔｉｔｌｅ Ｋｅｙ）２０として記録される。なお、スクランブル処理に関しては例えば、上述した図2に示したスクランブラー２００を適用可能である。

【００４０】また、記録されるＡＶコンテンツ２１はコンテンツ暗号化手段２２にて、記録する際に決められるタイトル毎に異なるタイトルキー１８（スクランブルされる前の）でスクランブルされた暗号化ＡＶコンテンツ（Ｅｎｃｒｙｐｔｅｄ ＡＶＣｏｎｔｅｎｔｓ）３１としてディスク２に記録される。なお、スクランブル処理に関しては例えば、上述した図2に示したスクランブラー２００を適用可能である。

【００４１】（３）再生装置

再生装置２３にもあらかじめ複数のデバイスキー５－１～５－ｎのうち１つ、例えば、デバイスキー２４（５－ｋ）が割り当てられている。上述したようにディスクキーブロック（ＤＫＢ７）は１つのディスクキー４を複数のデバイスキー５－１～５－ｎで暗号化（Ｅｎｃｒｙｐｔ）しているので再生装置２３のデバイスキー２４（５－ｋ）は、記録装置のデバイスキー１４（５－ｊ）と異なるデバイスキーでかまわない。

【００４２】再生装置２３は再生に先立ち、ディスク２一枚毎にユニークなデータ（ユニーク・メディア・ＩＤ）３を読み出すと共に、ディスク２の所定の領域に記録されている暗号化ＤＫＢ９を読み出す。

【００４３】再生装置２３にあるスクランブルディスクキー復号部（ＤＫＢ　Ｄｅｃｒｙｐｔｉｏｎ）２５では、ディスク２より読み出した二重にスクランブルされたディスクキー群９を、同じくディスク２より読み出したユニーク・メディア・ＩＤ３でデスクランブルしてディスクキー群(ディスクキーブロック（ＤＫＢ））２６（ＤＫＢ７に相当）を復元する。なお、上述したデスクランブルの処理には、例えば、上述した図３に示したデスクランブラー３００を適用することが可能である。

【００４４】次に再生装置２３にあるディスクキー復号部（Ｄｉｓｃ　Ｋｅｙ　Ｄｅｃｒｙｐｔｉｏｎ）２７で再生装置２３の持つデバイスキー２４でディスクキーブロック（ＤＫＢ）２６を復号してディスクキー２８（ディスクキー４に相当）を復元する。

【００４５】復号されたディスクキー２８は記録側で使ったディスク２一枚毎にユニークなディスクキー１７と一致させるため、ディスク２より読み出されたユニーク・メディア・ＩＤ３を用いてユニークメディアキー処理部（Ｐｒｏｃｅｓｓ　Ｕｎｉｑｕｅ　Ｍｅｄｉａ　Ｋｅｙ）２９で処理され、ユニークなディスクキー１７を得る。この処理には、例えば、上述した図５に示したＥＯＲ６０１による処理を適用することが可能である。この場合、鍵情報としてディスクキー２８を、媒体識別情報としてユニーク・メディア・ＩＤ３をＥＯＲ６０１に入力することによりユニークなディスクキー１７を復元することができる。

【００４６】次にディスク２に記録されている暗号化タイトルキー２０を読み出す。暗号化タイトルキー２０はユニークなディスクキー１７で暗号化されているので、ユニークメディアキー処理部（Ｐｒｏｃｅｓｓ　Ｕｎｉｑｕｅ　Ｍｅｄｉａ　Ｋｅｙ）２９より出力されるユニークなディスクキー１７を使ってタイトルキー復号部（Ｔｉｔｌｅ　Ｋｅｙ　Ｄｅｃｒｙｐｔｉｏｎ）３０において、暗号化タイトルキー２０を元々のタイトルキー１８に復号する。

【００４７】ディスク２から暗号化ＡＶコンテンツ３１を読み出し、暗号化ＡＶコンテンツ３１はタイトルキー１８でスクランブルされているので、コンテンツ復号部（Ｃｏｎｔｅｎｔｓ　Ｅｎｃｒｙｐｔｉｏｎ）３２は復号されたタイトルキー１８を使用してデスクランブを行いＡＶコンテンツ２１を得る。

【００４８】なお、上記説明におけるでスクランブラーはキーデータを初期値にＭ系列の乱数を発生させスクランブルしたいデータとＥＯＲをとることで処理を行う。これに対してデスクランブラーはスクランブラーと同様にキーデータを初期値にＭ系列の乱数を発生させスクランブルしたいデータとＥＯＲをとれば、Ｍ系列のデータはスクランブラーと同期がとれるためデータを復元することができる。また、ディスクキーをディスク一枚毎に異なるユニーク・メディア・ＩＤとＥＯＲをとればユニークなディスクキーが得られる。

【００４９】本発明は上述したようにディスク一枚毎にユニークなデータ（ユニーク・メディア・ＩＤ）が記録され、そのＩＤでスクランブルされた複数のディスクキー群(ＤＫＢ)が二重にスクランブルされているので、メディア上のスクランブルされたＤＫＢデータはディスク毎に異なる。したがって、データとして記録されたスクランブルされたコンテンツデータやタイトルキーデータがスクランブルされたＤＫＢデータを含んで別のディスクにディスク丸ごとコピーが行われたとしても、コピー先のユニーク・メディア・ＩＤはコピー元のユニーク・メディア・ＩＤと全く異なるため正しくディスクキーブロックは復元できない。正しくディスクキーブロックが復元できないとタイトルキーデータやスクランブルされたコンテンツデータは復元できないのでコピー防止になる。

【００５０】ＤＶＤ－ＲＡＭと異なりＤＶＤ－ＲＷのＭＫＢ記録領域は書き換え可能であるが、そこに書かれている二重に暗号化されたディスクキーブロックを改変するとしても、ユニーク・メディア・ＩＤと二重に暗号化されたディスクキーブロックの関係（暗号のアルゴリズム）がわからない限り正しく改変されたディスクキーブロックデータは得られない。つまりメディア上は全ての領域で書き換え可能なＤＶＤ－ＲＷ媒体で技術的見通しが立っていないＥｍｂｏｓｓ－ｐｉｔｔを使わずにＤＶＤ－ＲＡＭと同じコピー防止が実現できる。

【００５１】本発明は上述したような構成であるので、ＤＶＤ－ＲＡＭの様なＲＯＭの領域とＲＡＭの領域の性能を両立させ、かつ性能の両立をさせるような特殊な構造のメディアとする必要が無く、メディア上は全ての領域で書き換え可能な（Ｕｎｉｑｕｅ　Ｍｅｄｉａ　ＩＤ領域を除き）ままで書き換え可能な媒体のコピー防止が実現でき、またメディア上は全ての領域で書き換え可能な領域なので、ＲＯＭの領域とＲＡＭの領域で規格を分ける必要も無く、さらに、例えば、ＢＣＡ等のＵｎｉｑｕｅ　Ｍｅｄｉａ　ＩＤによりディスクキーブロックが二重にスクランブルされたデータはディスク毎に異なるので、ＤＫＢ領域を含むディスク丸ごとコピーが行われ

ても正しくディスクキーブロックは復元できないのでコンテンツデータは復元できない。つまり、一枚一枚のディスクに記録されるのはスクランブルされたＤＫＢだから従来のような裸のＤＫＢデータを記録する場合に比べてハッキングに対する強度が増す。さらに、ディスクキーブロックを使用しているので記録機、再生機でデバイスキーが異なっていても構わない。

【００５２】

【発明の効果】本発明は上述したような構成であるので、書き換え可能な媒体のコピー防止を実現でき、記録されたデータはディスク毎に異なるのでディスク丸ごとコピーが行われたとしてもコンテンツデータは正しく復元できないので、強力なコピープロテクトが可能となり、さらに、ディスクキーブロックを使用しているので記録機、再生機でデバイスキーが異なっていても正規の再生は可能になるという利点を有する。

【００５３】

【図面の簡単な説明】

【図１】本発明の実施例を示す図である。

【図２】スクランブラーの一例を示す図である。

【図３】デスクランブラーの一例を示す図である。

【図４】ＰＮ乱数発生部の一例を示す図である。

【図５】演算処理の一例を示す図である。

【図６】ＣＳＳのＤＶＤ－Ｖｉｄｅｏ（ＲＯＭ）への適用例を示す図である。

【図７】ＤＶＤ－ＲＡＭのコピーガードを説明する図である。

【図８】ビットバイビットコピーを説明するための図である。

【図９】ディスクの物理レイアウトを示す図である。

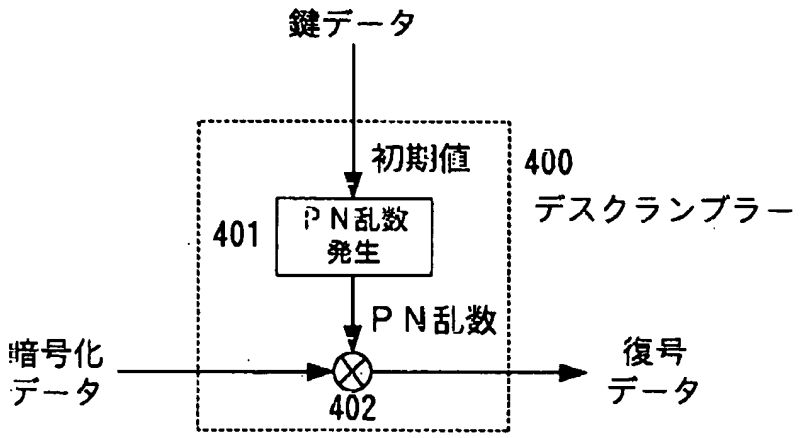
【図１０】初期値「００００」のときのＰＮ乱数発生手段３０１の出力を示す図である。

【図１１】初期値「１００１」のときのＰＮ乱数発生手段３０１の出力を示す図である。

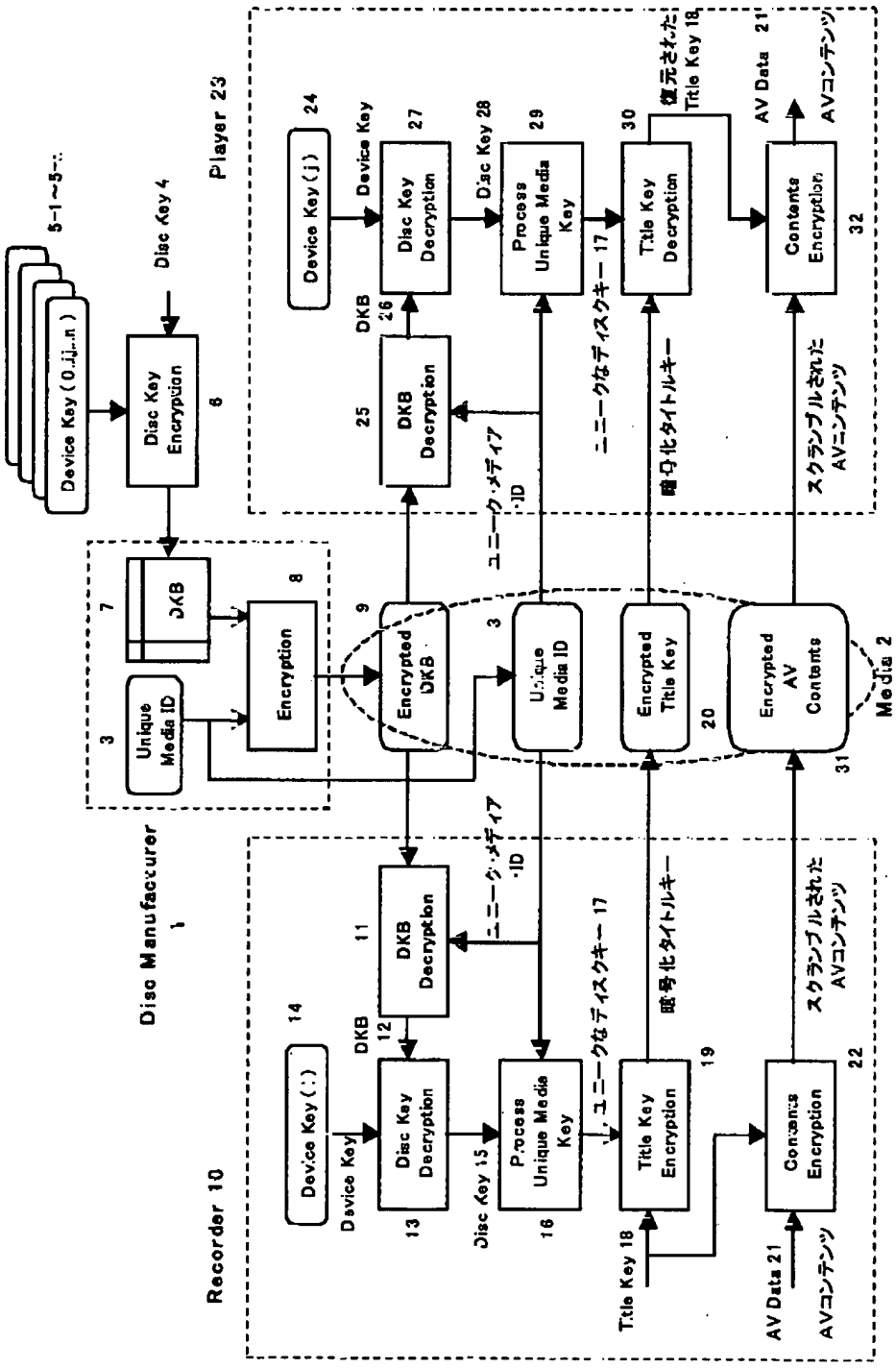
【符号の説明】

１…ディスク製造者
２…ディスク
３…ユニーク・メディア・ＩＤ
４…ディスクキー
５－１～５－ｎ…デバイスキー
６…ディスクキー暗号化手段
７…ディスクキーブロック（ＤＫＢ）
８…暗号手段
９…暗号化ＤＫＢ
１０…記録機
１１…ＤＫＢ復号手段
１２…ＤＫＢ
１３…ディスクキー復号手段
１４…デバイスキー
１５…ディスクキー
１６…ユニークメディアキー処理手段
１７…ユニークディスクキー
１８…タイトルキー
１９…タイトル暗号手段
２０…暗号化タイトルキー
２１…ＡＶコンテンツ
２２…コンテンツ暗号手段
２３…再生機
２４…デバイスキー
２５…ＤＫＢ復号手段
２６…ＤＫＢ
２７…ディスクキー復号手段
２８…ディスクキー
２９…ユニークメディアキー処理手段
３０…タイトルキー復号手段
３１…暗号化ＡＶコンテンツ
３２…ＡＶコンテンツ復号手段

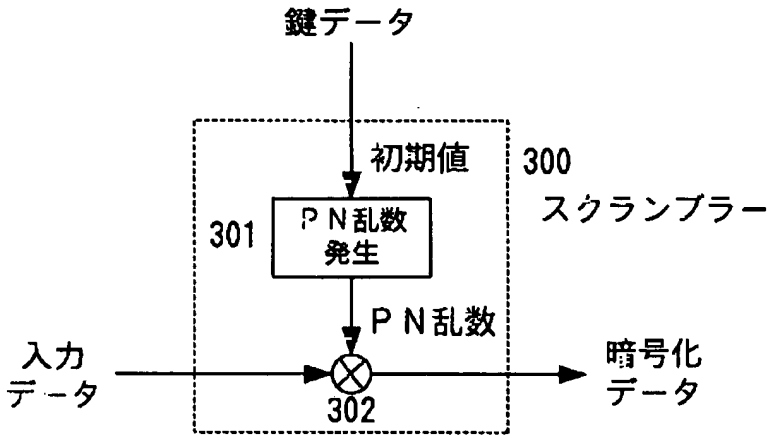
【図３】



【図1】


Disc Manufacturer 1
Recorder 10
Player 23
Media 2
Device Key (1..n)
Disc Key 4
Disc Key Encryption 6
DKB 7
Unique Media ID 3
Encryption 8
Encrypted DKB 9
Unique Media ID 3
Encrypted Title Key 20
Encrypted AV Contents 31
DKB Decryption 11
DKB Decryption 25
Device Key (1) 14
Device Key 24
Disc Key Decryption 13
Disc Key Decryption 27
Process Unique Media Key 16
Disc Key 15
Process Unique Media Key 29
Disc Key 28
Title Key Encryption 19
Title Key Decryption 30
Title Key 18
Contents Encryption 22
Contents Encryption 32
AV Data 21
AVコンテンツ
ユニークなディスクキー 17
暗号化タイトルキー
スクランブルされたAVコンテンツ
復元されたTitle Key 18

【図２】



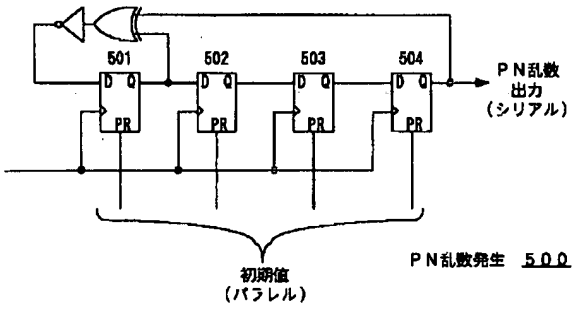
【図１０】

初期値＝「0000」

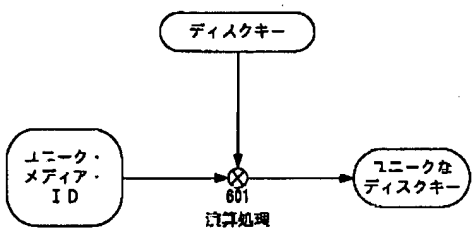
クロック数	レジスター値	出力	データ	スクランブル出力
0	0000	0	0	0
1	1000	0	0	0
2	0100	0	0	0
3	1010	0	0	0
4	0101	1	1	0
5	0010	0	0	0
6	1001	1	0	1
7	1100	0	0	0
8	0110	0	0	0
9	1011	1	1	0
10	1101	1	0	1
11	1110	0	0	0
12	0111	1	1	0
13	0011	1	1	0
14	0001	1	0	1
15	0000	0	0	0
16	1000	0	0	0
17	0100	0	0	0
18	1010	0	1	1
19	0101	1	0	1
20	0010	0	1	1
21	1001	1	0	1
22	1100	0	1	1
23	0110	0	0	0

MSB

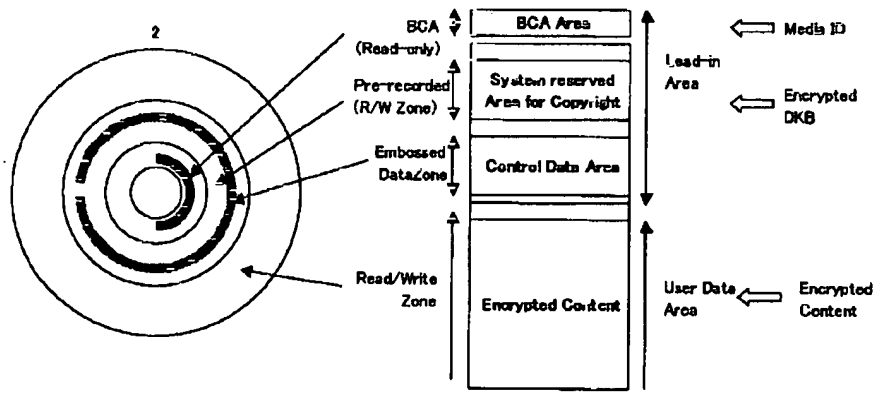
【図４】



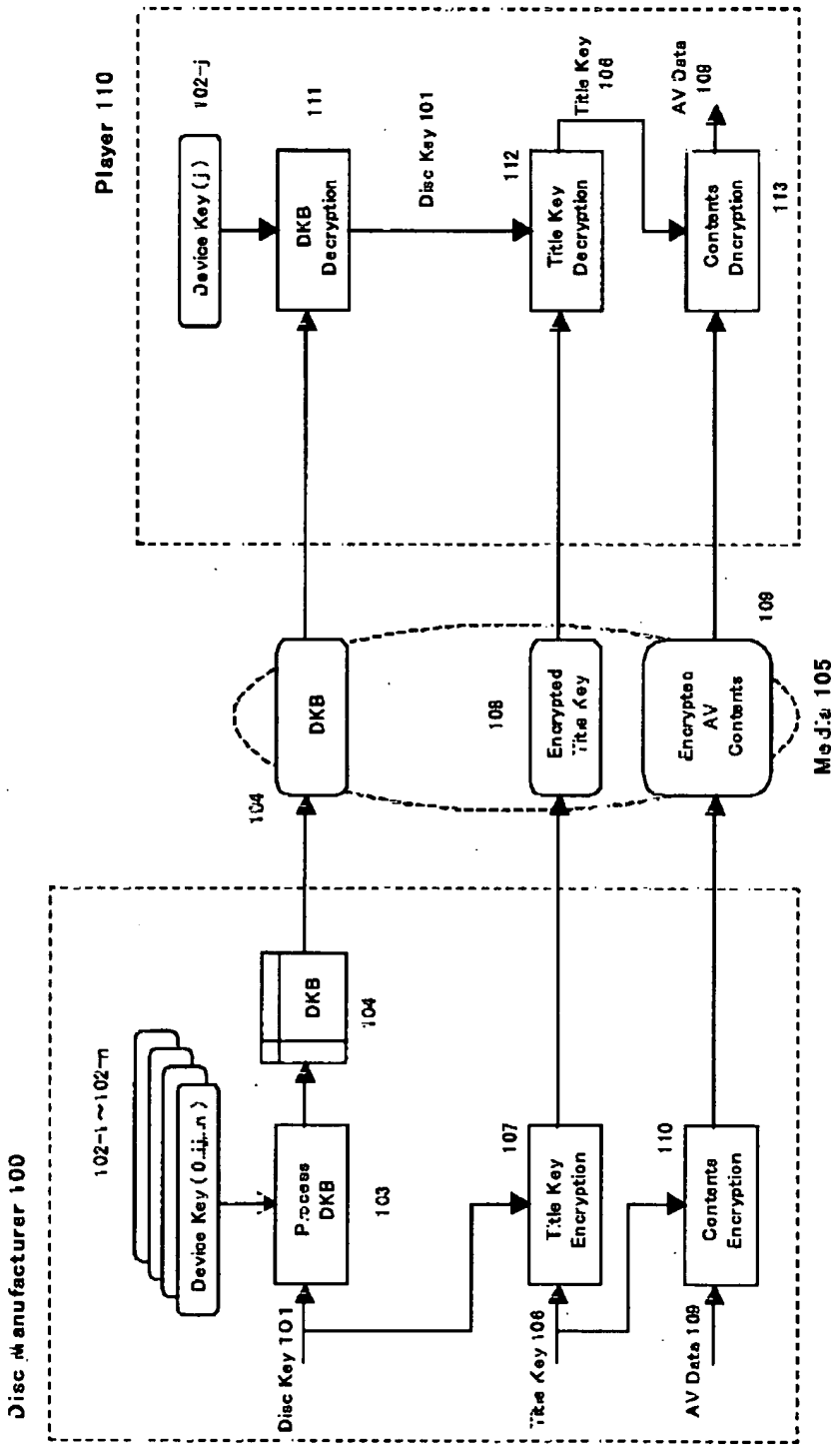
【図５】



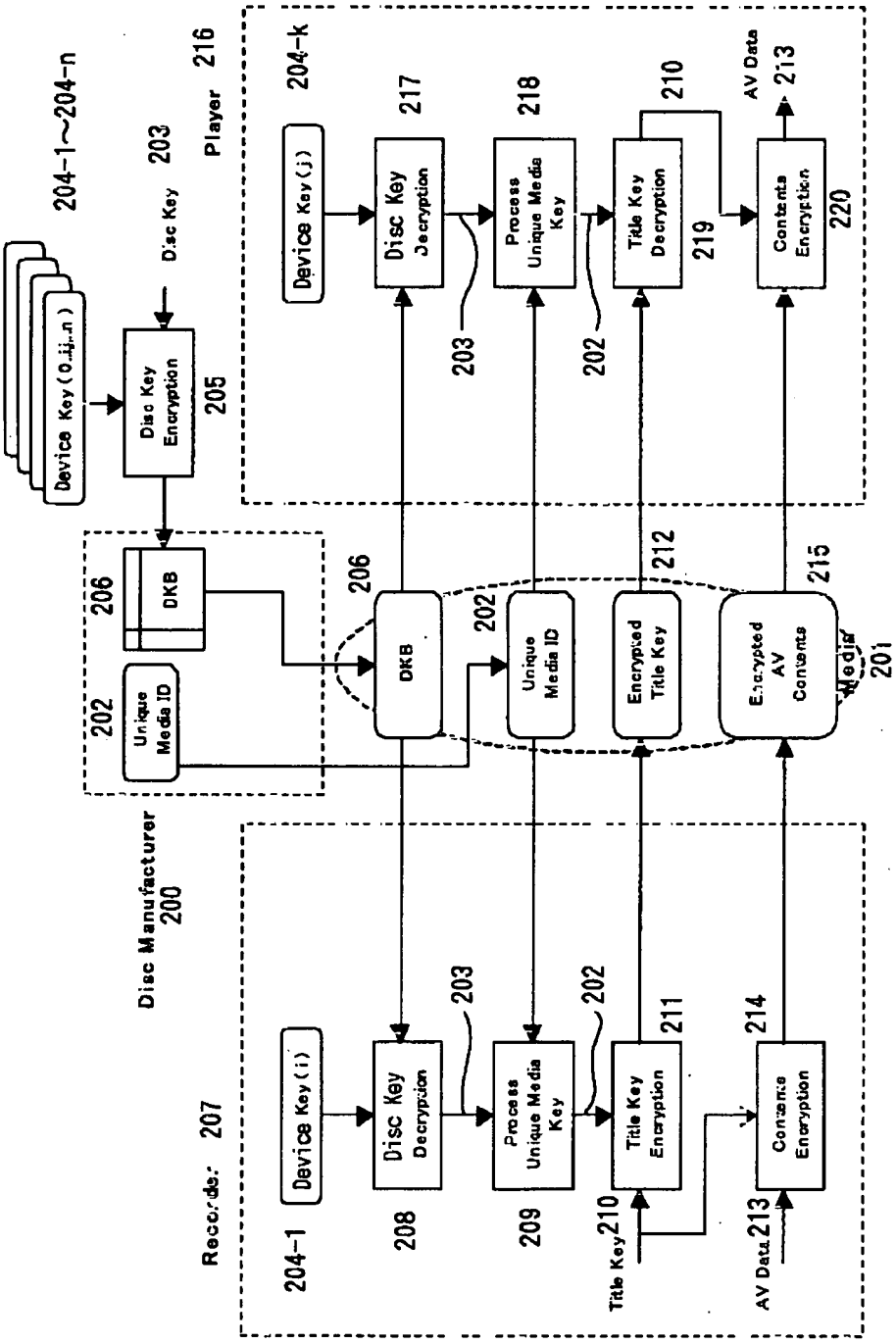
【図８】



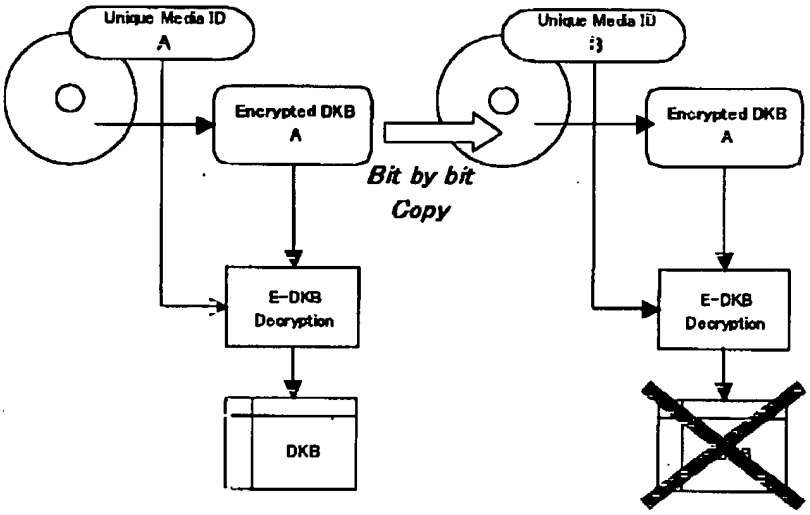
【図6】


Player 110
Device Key (j)
102-j
DKB Decryption
111
Disc Key 101
Title Key Decryption
112
Title Key 106
AV Data 108
Contents Dncryption
113
DKB
104
Encrypted Title Key
108
Encrypted AV Contents
109
Media 105
Disc Manufacturer 100
Device Key (1...n)
102-1~102-n
Process DKB
103
Title Key Encryption
107
Contents Encryption
110
Disc Key 101
Title Key 106
AV Data 108

【図7】


Player 216
Disc Manufacturer 200
Recorder 207
Device Key(j)
Disc Key Decryption
Process Unique Media Key
Title Key Decryption
Contents Encryption
AV Data
Device Key(0...j...n)
Disc Key
Disc Key Encryption
DKB
Unique Media ID
Encrypted Title Key
Encrypted AV Contents
Media
Device Key(i)
Title Key Encryption
Title Key
204-1~204-n
204-k
204-1
201
202
203
205
206
207
208
209
210
211
212
213
214
215
217
218
219
220

【図9】



【図11】

初期値＝「1001」

クロック数	レジスター値	出力	データ	スクランブル出力
0	1001	1	0	1
1	1100	0	0	0
2	0110	0	0	0
3	1011	1	0	1
4	1101	1	1	0
5	1110	0	0	0
6	0111	1	0	1
7	0011	1	0	1
8	0001	1	0	1
9	0000	0	1	1
10	1000	0	0	0
11	0100	0	0	0
12	1010	0	1	1
13	0101	1	1	0
14	0010	0	0	0
15	1001	1	0	1
16	1100	0	0	0
17	0110	0	0	0
18	1011	1	1	0
19	1101	1	0	1
20	1110	0	1	1
21	0111	1	0	1
22	0011	1	1	0
23	0001	1	0	1

MSB